PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-108910A**

(43)Date of publication of application : **12.04.2002**

(51)Int.Cl. **G06F 17/30**

// G09C 1/00

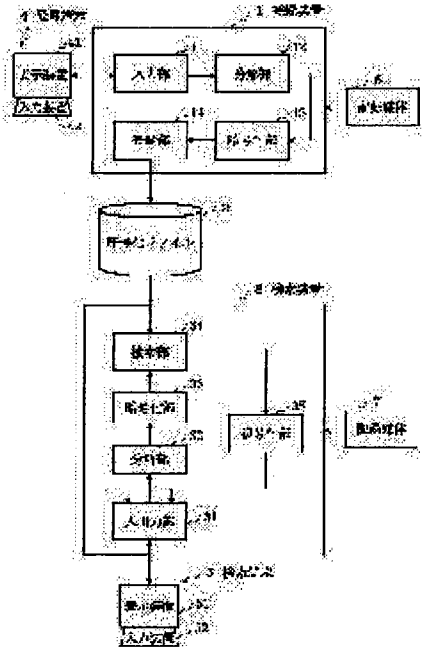
(21)Application number : **2000-294010**

(22)Date of filing : **27.09.2000**

(71)Applicant : **NEC SOFT LTD**

(72)Inventor : **HAMADA TOSHIHIRO**

(54) ENCIPHERED FILING SYSTEM, ENCIPHERED FILE RETRIEVING METHOD AND COMPUTER READABLE RECORDING MEDIUM



(57)Abstract:

PROBLEM TO BE SOLVED: To provide an enciphered filing system and an enciphered file retrieving method capable of partial-coincidence retrieval in an enciphered state.

SOLUTION: A register 1 registers a record, with which a key item to become a key in the case of retrieval is enciphered at least among plural items, in an enciphered file 2. In that case, by enciphering and coupling the data of the key item for each unit character, the register 1 generates the enciphered data of the entire key item. While using an enciphered retrieve key, with which the retrieve key applied as a retrieval condition is enciphered and coupled for each unit character, a retrieving device 3 executes complete-coincidence retrieval and partial-coincidence retrieval of the enciphered file 2.

D2

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－108910
（P2002－108910A）
(43)公開日　平成14年４月12日(2002.4.12)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード(参考)
Ｇ０６Ｆ　17/30	３２０	Ｇ０６Ｆ　17/30	３２０Ｃ　５Ｂ０７５
	２１０		２１０Ｚ　５Ｊ１０４
// Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ

審査請求　有　　請求項の数16　ＯＬ　（全　９　頁）

(21)出願番号　特願2000－294010(P2000－294010)

(22)出願日　平成12年９月27日(2000.9.27)

(71)出願人　000232092
エヌイーシーソフト株式会社
東京都江東区新木場一丁目18番６号

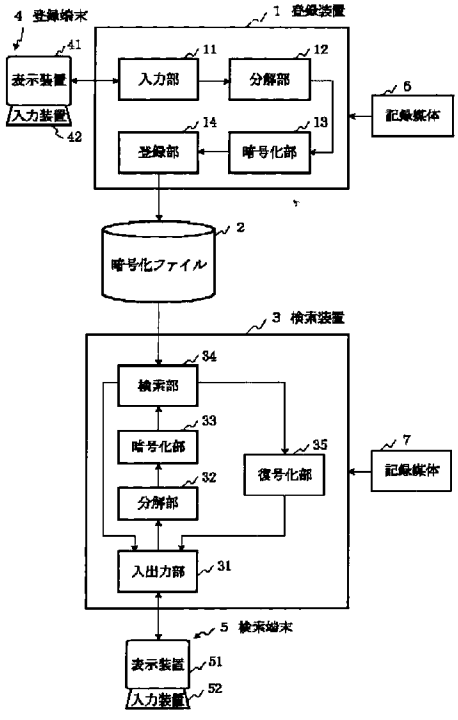
(72)発明者　濱田　智弘
東京都江東区新木場一丁目18番６号　エヌイーシーソフト株式会社内

(74)代理人　100088959
弁理士　境　廣巳

Ｆターム(参考)　5B075 ND01 NK01 QM10
5J104 AA01 CA02 NA02

(54)【発明の名称】　暗号化ファイルシステム及び暗号化ファイル検索方法並びにコンピュータ可読記録媒体

(57)【要約】
【課題】　暗号化された状態で部分一致検索が行える暗号化ファイルシステム及び暗号化ファイル検索方法を提供する。
【解決手段】　登録装置１は、複数の項目のうち少なくとも検索する際のキーとなるキー項目を暗号化したレコードを暗号化ファイル２に登録する。その際、登録装置１は、キー項目のデータを単位文字毎に暗号化して結合することにより、キー項目全体の暗号化データを生成する。検索装置３は、検索条件として与えられた検索キーを単位文字毎に暗号化して結合した暗号化検索キーを用いて暗号化ファイル２に対して完全一致検索および部分一致検索を実行する。



1

【特許請求の範囲】

【請求項１】　複数の項目のうち少なくとも検索する際のキーとなるキー項目を暗号化したレコードであって、キー項目の暗号化はキー項目のデータを単位文字毎に暗号化しそれを結合することによって行われているレコードを格納するファイルと、

検索条件として与えられた検索キーを単位文字毎に暗号化して結合した暗号化検索キーを用いて前記ファイルを検索する検索装置とを備えた暗号化ファイルシステム。

【請求項２】　前記検索装置は、検索キーを単位文字に分解する分解手段と、分解して得られた個々の単位文字毎に暗号化して結合することにより暗号化検索キーを生成する暗号化手段とを含む請求項１記載の暗号化ファイルシステム。

【請求項３】　前記検索装置は、暗号化検索キーと完全一致または部分一致するキー項目を持つレコードを前記ファイルから検索する検索手段を含む請求項１または２記載の暗号化ファイルシステム。

【請求項４】　前記検索装置は、前記ファイルから検索したレコードを復号化して検索結果として出力する復号化手段を含む請求項３記載の暗号化ファイルシステム。

【請求項５】　複数の項目のうち少なくとも検索する際のキーとなるキー項目を暗号化したレコードを前記ファイルに登録する装置であって、キー項目の暗号化は、キー項目のデータを単位文字毎に暗号化して結合することにより行う登録装置を備えた請求項１、２、３または４記載の暗号化ファイルシステム。

【請求項６】　前記登録装置は、登録対象となるレコードのキー項目のデータを単位文字に分解する分解手段と、分解して得られた個々の単位文字毎に暗号化して結合することによりキー項目全体を暗号化する暗号化手段とを含む請求項５記載の暗号化ファイルシステム。

【請求項７】（ａ）複数の項目のうち少なくとも検索する際のキーとなるキー項目を暗号化したレコードをファイルに登録するステップであって、キー項目の暗号化は、キー項目のデータを単位文字毎に暗号化して結合することにより行うステップと、（ｂ）検索条件として与えられた検索キーを単位文字毎に暗号化して結合した暗号化検索キーを用いて前記ファイルを検索するステップとを含む暗号化ファイル検索方法。

【請求項８】　前記ステップｂは、検索キーを単位文字に分解するステップと、分解して得られた個々の単位文字毎に暗号化して結合することにより暗号化検索キーを生成するステップとを含む請求項７記載の暗号化ファイル検索方法。

【請求項９】　前記ステップｂは、暗号化検索キーと完全一致または部分一致するキー項目を持つレコードを前記ファイルから検索するステップを含む請求項７または８記載の暗号化ファイル検索方法。

【請求項１０】　前記ステップｂは、前記ファイルから

2

検索したレコードを復号化して検索結果として出力するステップを含む請求項９記載の暗号化ファイル検索方法。

【請求項１１】　前記ステップａは、登録対象となるレコードのキー項目のデータを単位文字に分解するステップと、分解して得られた個々の単位文字毎に暗号化して結合することによりキー項目全体を暗号化するステップとを含む請求項７、８、９または１０記載の暗号化ファイル検索方法。

【請求項１２】　コンピュータを、複数の項目のうち少なくとも検索する際のキーとなるキー項目を暗号化したレコードを前記ファイルに登録する手段であって、キー項目の暗号化は、キー項目のデータを単位文字毎に暗号化して結合することにより行う登録装置、

検索条件として与えられた検索キーを単位文字毎に暗号化して結合した暗号化検索キーを用いて前記ファイルを検索する検索装置、として機能させるプログラムを記録したコンピュータ可読記録媒体。

【請求項１３】　前記検索装置は、検索キーを単位文字に分解する分解手段と、分解して得られた個々の単位文字毎に暗号化して結合することにより暗号化検索キーを生成する暗号化手段とを含む請求項１２記載のコンピュータ可読記録媒体。

【請求項１４】　前記検索装置は、暗号化検索キーと完全一致または部分一致するキー項目を持つレコードを前記ファイルから検索する検索手段を含む請求項１２または１３記載のコンピュータ可読記録媒体。

【請求項１５】　前記検索装置は、前記ファイルから検索したレコードを復号化して検索結果として出力する復号化手段を含む請求項１４記載のコンピュータ可読記録媒体。

【請求項１６】　前記登録装置は、登録対象となるレコードのキー項目のデータを単位文字に分解する分解手段と、分解して得られた個々の単位文字毎に暗号化して結合することによりキー項目全体を暗号化する暗号化手段とを含む請求項１５記載のコンピュータ可読記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はデータを暗号化して格納する暗号化ファイルシステム及び暗号化ファイル検索方法に関する。

【０００２】

【従来の技術】インターネットの普及に伴い、各種の情報がインターネット上で数多く提供されている。その反面、情報を提供する側としては、個人情報や企業情報等の提供すべきでない情報までもがインターネット上に漏れてしまう、或いは盗まれてしまうというセキュリティ面での危険性も有している。漏れた場合あるいは盗まれた場合に備えて、データベースのファイルを暗号化しておく技術がある。一方で、データベースのファイルの情

報は、企業内の必要不可欠な人達へは提供する必要があり、暗号化ファイルに対する検索技術が必要となってくる。

【０００３】暗号化ファイルに対する最も単純な検索手法は、暗号化ファイルの内容を全て復号化して同一構造の別のデータベースのファイルに格納し、そのファイルからデータの検索を行う手法である。以下、この手法を第１の従来技術と呼ぶ。

【０００４】暗号化ファイルに対する別の検索手法が特開２０００－１１００１号公報に記載されている。この従来手法では、平文で入力された検索キーワードを暗号化して暗号化ファイルを検索する。具体的には、予め暗号化された複数のファイルを復号化して、各ファイルに含まれるキーワードとそのキーワードが含まれていたファイル名との組を抽出し且つ各組中のキーワードを暗号化したインデックスを生成する。例えば「鈴木一郎」というキーワードが或るファイルＡに含まれていた場合、「鈴木一郎」を暗号化したデータとファイルＡの名前との組を生成する。暗号化されたデータは一般にランダムなデータ列となり、表記が困難なので、本明細書では便宜上、アルファベット文字列で表記する。例えば「鈴木一郎」は「ｚｄｓｉｕｋｉｉｏ」に暗号化されたとする。次に、利用者から検索キーワードとして「鈴木一郎」が入力された場合、それを暗号化して「ｚｄｓｉｕｋｉｉｏ」なる暗号化検索キーワードを生成し、インデックス中の暗号化キーワードと照合して、ファイルＡの名前を抽出する。以下、この手法を第２の従来技術と呼ぶ。

【０００５】

【発明が解決しようとする課題】第１の従来技術では、復号化したデータがデータベースに存在することになるため、セキュリティ面からみると危険性が伴ってしまう。

【０００６】他方、第２の従来技術では暗号化された状態で検索を行うためファイルのデータの機密性は確保されるが、部分一致検索が行えないという課題がある。その理由は、或る長さの文字列全体を暗号化したデータ中には、その文字列の一部分を暗号化したデータは含まれないからである。例えば個人情報を検索する際に、個人を特定する氏名だけでなく、氏だけを検索キーに使う場合が考えられる。この場合、暗号化ファイルのキー項目が氏名である場合、従来手法では「氏名」全体を一括に暗号化して登録し、或る検索キーが入力された場合に検索キー全体を一括に暗号化した暗号化検索キーで検索を行う。しかし、前述したように例えば氏名「鈴木一郎」全体を一括に暗号化した「ｚｄｓｉｕｋｉｉｏ」中には、氏「鈴木」だけを暗号化したデータは含まれないため、そのような部分一致検索は行えない。

【０００７】本発明はこのような従来の問題点を解決したもので、その目的は、暗号化された状態で部分一致検索が行える暗号化ファイルシステム及び暗号化ファイル検索方法を提供することにある。

【０００８】

【課題を解決するための手段】本発明の暗号化ファイルシステムは、複数の項目のうち少なくとも検索する際のキーとなるキー項目を暗号化したレコードであって、キー項目の暗号化はキー項目のデータを単位文字毎に暗号化しそれを結合することによって行われているレコードを格納するファイルと、検索条件として与えられた検索キーを単位文字毎に暗号化して結合した暗号化検索キーを用いて前記ファイルを検索する検索装置とを備えている。

【０００９】また、前記検索装置は、検索キーを単位文字に分解する分解手段、分解して得られた個々の単位文字毎に暗号化して結合することにより暗号化検索キーを生成する暗号化手段、暗号化検索キーと完全一致または部分一致するキー項目を持つレコードを前記ファイルから検索する検索手段、前記ファイルから検索したレコードを復号化して検索結果として出力する復号化手段を含んでいる。

【００１０】また、本発明の暗号化ファイルシステムは、複数の項目のうち少なくとも検索する際のキーとなるキー項目を暗号化したレコードを前記ファイルに登録する装置であって、キー項目の暗号化は、キー項目のデータを単位文字毎に暗号化して結合することにより行う登録装置を備えている。また、この登録装置は、登録対象となるレコードのキー項目のデータを単位文字に分解する分解手段と、分解して得られた個々の単位文字毎に暗号化して結合することによりキー項目全体を暗号化する暗号化手段とを含んでいる。

【００１１】また、本発明の暗号化ファイル検索方法は、（ａ）複数の項目のうち少なくとも検索する際のキーとなるキー項目を暗号化したレコードをファイルに登録するステップであって、キー項目の暗号化は、キー項目のデータを単位文字毎に暗号化して結合することにより行うステップと、（ｂ）検索条件として与えられた検索キーを単位文字毎に暗号化して結合した暗号化検索キーを用いて前記ファイルを検索するステップとを含んでいる。

【００１２】また、前記ステップｂは、検索キーを単位文字に分解するステップと、分解して得られた個々の単位文字毎に暗号化して結合することにより暗号化検索キーを生成するステップと、暗号化検索キーと完全一致または部分一致するキー項目を持つレコードを前記ファイルから検索するステップと、前記ファイルから検索したレコードを復号化して検索結果として出力するステップとを含んでいる。

【００１３】また、前記ステップａは、登録対象となるレコードのキー項目のデータを単位文字に分解するステップと、分解して得られた個々の単位文字毎に暗号化し

て結合することによりキー項目全体を暗号化するステップとを含んでいる。

【００１４】

【作用】本発明にあっては、ファイルに暗号化したレコードを登録する際、キー項目のデータを単位文字毎に暗号化し結合して登録しておく。そして、検索時には検索キーを単位文字毎に暗号化し結合した暗号化検索キーを用いてファイルを検索する。

【００１５】

【発明の実施の形態】次に本発明の実施の形態の例について図面を参照して詳細に説明する。

【００１６】図１は本発明の暗号化ファイルシステムの一例を示すブロック図であり、登録装置１、暗号化ファイル２、検索装置３、登録端末４及び検索端末５で構成されている。

【００１７】暗号化ファイル２は、図２に示すような複数の項目Ｃ０～Ｃｍを持つレコードＲ１～Ｒｎの集合で構成される。各レコードＲ１～Ｒｎは、例えば特定の個人に対応しており、その個人の各種の情報を保持している。例えば項目Ｃ１は氏名（漢字）、項目Ｃ２は氏名（カタカナ）、項目Ｃｍは年収などを示す。他に、所属部署や役職など各種のデータが他の項目に格納されている。また、項目Ｃ０のレコード番号は当該レコードを一意に識別するレコード識別子である。各レコードＲ１～Ｒｎは、少なくとも検索する際のキーとなるキー項目が暗号化されている。ここでは、説明の便宜上、項目Ｃ１と項目Ｃ２がキー項目であり、キー項目以外の項目で暗号化されている項目は項目Ｃｍだけを想定する。つまり、項目Ｃ０～Ｃｍのうち、項目Ｃ１、Ｃ２、Ｃｍは暗号化されており、残りの項目Ｃ３～Ｃｍ－１は暗号化されていないものとする。

【００１８】登録装置１は暗号化ファイル２にレコードを登録する装置である。登録装置１は、登録するレコードのキー項目Ｃ１、Ｃ２の暗号化は、キー項目Ｃ１、Ｃ２のデータ全体を一括して暗号化するのではなく、キー項目Ｃ１、Ｃ２のデータを単位文字毎に暗号化し、それを結合することによって行う。

【００１９】登録装置１は、図１に示されるように、登録対象となるレコードを外部から入力する入力部１１と、入力されたレコード中のキー項目Ｃ１、Ｃ２のデータを単位文字に分解する分解部１２と、入力されたレコード中の暗号化すべき項目Ｃ１、Ｃ２、Ｃｍを暗号化する暗号化部１３と、暗号化されたレコードを暗号化ファイル２に登録する登録部１４とから構成される。ここで、暗号化部１３は、暗号化すべき項目がキー項目Ｃ１、Ｃ２の場合、分解部１２によって分解された単位文字毎に独立に暗号化を行い、その結果を連結することにより、当該キー項目Ｃ１、Ｃ２全体の暗号化データを生成する。また、暗号化すべき項目がキー項目以外の項目Ｃｍの場合、当該キー項目Ｃｍ全体を一括して暗号化する。暗号化には任意の暗号手法を採用することができ、暗号化の鍵も公開鍵、共通鍵の任意の鍵を使用することができる。本実施例では、暗号鍵は登録部１に事前に設定されているものとする。

【００２０】登録装置１は、パーソナルコンピュータやワークステーション・サーバ等のコンピュータを構成する中央処理装置、主記憶及び制御プログラムによって構成することができる。この場合、制御プログラムはＣＤ－ＲＯＭ、半導体メモリ、磁気ディスク等の機械読み取り可能な記録媒体６に記憶されており、登録装置１を構成するコンピュータの立ち上げ時などにコンピュータに読み取られ、そのコンピュータの動作を制御することにより、そのコンピュータ上に入力部１１、分解部１２、暗号化部１３及び登録部１４を実現する。

【００２１】登録端末４は、暗号化ファイル２に登録するレコードを平文で作成して登録装置１にその登録を要求する際に利用者が使用する装置であり、表示装置４１と入力装置４２とを備えている。利用者は、表示装置４１の画面上でレコードの内容を編集し、入力装置４２からの指示でその登録を登録装置１に要求する。

【００２２】検索端末５は、暗号化ファイル２に対する検索時に利用者が使用する装置であり、表示装置５１と入力装置５２とを備えている。利用者は、表示装置５１の画面上で検索キーとなる文字列などの検索条件を編集し、入力装置５２からの指示でその検索条件に基づく検索を検索装置３に要求する。

【００２３】検索装置３は、利用者から入力された検索条件に合致するレコードを暗号化ファイル２から検索して利用者に提示する装置である。検索装置３は、利用者から入力された検索キーを暗号化した暗号化検索キーを使って暗号化ファイル２の検索を行う。その際、検索キー全体を一括して暗号化した暗号化検索キーを使うのではなく、検索キーを単位文字毎に暗号化し、それを結合した暗号化検索キーを使う。

【００２４】検索装置３は、図１に示されるように、検索端末５とデータの授受を行う入出力部３１と、入出力部３１を通じて入力された検索条件中の検索キーを単位文字に分解する分解部３２と、分解部３２で分解された単位文字毎に独立に暗号化を行い、その結果を連結することにより暗号化検索キーを生成する暗号化部３３と、暗号化部３３で生成された暗号化検索キーを使って検索条件を満たすレコードを暗号化ファイル２から検索する検索部３４と、検索部３４で検索されたレコードを利用者に提示するために復号化する復号化部３５とから構成される。ここで、暗号化部３３では登録装置１がキー項目を暗号化した場合と同じ暗号手法で暗号化を行う。また、その暗号化に必要な暗号鍵は検索装置３に事前に設定されているものとする。同様に復号化部３５で必要な復号鍵も検索装置３に事前に設定されているものとする。

【００２５】検索装置３は、パーソナルコンピュータやワークステーション・サーバ等のコンピュータを構成する中央処理装置、主記憶及び制御プログラムによって構成することができる。この場合、制御プログラムはＣＤ－ＲＯＭ、半導体メモリ、磁気ディスク等の機械読み取り可能な記録媒体７に記憶されており、検索装置３を構成するコンピュータの立ち上げ時などにコンピュータに読み取られ、そのコンピュータの動作を制御することにより、そのコンピュータ上に入出力部３１、分解部３２、暗号化部３３、検索部３４及び復号化部３５を実現する。

【００２６】次に、本実施例の暗号化ファイルシステムの動作を説明する。先ず、暗号化ファイル２へのレコード登録時の動作を説明する。

【００２７】登録者は、先ず登録端末４を操作して、暗号化ファイル２へ登録するレコードの内容を表示装置４１の画面上で編集する。図３に表示装置４１に表示される登録画面４１１の一例を示す。登録画面４１１において、入力欄４１１－１～４１１－ｍは登録対象となるレコードの項目Ｃ１、項目Ｃ２、…、項目Ｃｍの内容を入力する欄である。利用者は入力装置４２から各入力欄４１１－１～４１１－ｍにそれぞれデータを入力していく。図示の例では、項目Ｃ１の入力欄４１１－１に漢字４文字からなる「鈴木一郎」が、項目Ｃ２の入力欄４１１－２にカタカナ７文字からなる「スズキイチロウ」が、項目Ｃｍの入力欄４１１－ｍに１０進数７桁の数値が、それぞれ入力されている。図示は省略しているが、項目Ｃ３～項目Ｃｍ－１に対応する入力欄にもデータを入力する。登録ボタン４１２は、編集し終えたレコードの登録を登録装置１に指示するボタンである。この登録ボタン４１２によって登録が指示されると、登録装置１は図４に示す処理を開始する。

【００２８】先ず登録装置１の入力部１１は、登録端末４の登録画面４１１上の入力欄４１１－１～４１１－ｍに設定されたデータを、登録対象レコードの項目Ｃ１～Ｃｍの値として入力する（Ｓ１）。次に分解部１２は、キー項目となる項目Ｃ１、Ｃ２毎に、そのデータを単位文字に分解する（Ｓ２）。キー項目以外の項目のデータはこのような分解処理は行わない。

【００２９】図５（ａ）に、項目Ｃ１のデータ「鈴木一郎」と、項目Ｃ２のデータ「スズキイチロウ」を、単位文字に分解した結果を示す。このようにキー項目のデータは、登録画面４１１に表示されている１文字を単位に分解される。ここでは、日本語を例に挙げたが、外国語の場合も同様であり、例えば英語の「Ｈｅｎｒｙ」は図５（ｂ）に示すようにアルファベット文字の１文字単位に分解される。また、ドイツ語のウムラウトのような特殊な文字も同様に、図５（ｃ）に例示するように１つの単位文字として抽出される。

【００３０】次に暗号化部１３は、登録対象レコードの項目Ｃ１～Ｃｍのうち、暗号化すべき項目Ｃ１、Ｃ２、Ｃｍをそれぞれ暗号化する（Ｓ３）。その際、キー項目Ｃ１、Ｃ２については、分解された単位文字毎に独立に暗号化を行い、暗号化されたデータを元の単位文字の並びと同じ順に結合することで、全体の暗号化データを生成する。他方、キー項目以外の項目のデータは、それ全体を一括して暗号化する。

【００３１】図６に単位文字に分解された「スズキイチロウ」を例にキー項目の暗号化の様子を示す。先ず、同図（ａ）に示すように、各単位文字毎に独立に暗号化し、各単位文字毎の暗号化データＢ、ｒ、ｇ、ｅ、ａ、￥、４を生成する。次に、同図（ｂ）に示すように、暗号化データを結合し、「スズキイチロウ」全体の暗号化データ「Ｂｒｇｅａ￥４」を生成する。なお、各暗号化データＢ、ｒ、ｇ、ｅ、ａ、￥、４はそれぞれ１単位の暗号化データであり、ランダムなデータ列である。そのデータ長は暗号化方式に依存し、可変長または固定長となる。１単位の暗号化データの先頭部分には暗号化データの開始を示す所定のビット列が置かれ、最後尾部分には暗号化データの終了を示す所定のビット列が置かれる。

【００３２】次に登録部１４は、暗号化部１３によって暗号化すべき項目Ｃ１、Ｃ２、Ｃｍが暗号化され且つそれ以外の項目Ｃ３～Ｃｍ－１は暗号化されていない状態の登録対象レコードに対し、暗号化ファイル２中で一意となる項目Ｃ０のレコード番号を付加して、暗号化ファイル２に登録する（Ｓ４）。

【００３３】次に暗号化ファイル２を検索する際の動作を説明する。検索者は、検索端末５を操作して、先ず検索条件を入力する。図７に表示装置５１に表示される検索画面５１１の一例を示す。この検索画面５１１は、カタカナ表記で氏名、または氏だけ、または名だけを項目Ｃ２の検索キーに指定し、完全一致検索または部分一致検索を要求するための検索画面の例であり、氏の入力欄５１２及び名の入力欄５１３と、検索ボタン５１４とが設けられている。検索者は、入力装置５２から入力欄５１２、５１３に検索キーとする任意のデータをカタカナで入力していく。図示の例では、氏の入力欄５１２に「スズキ」を入力し、名の入力欄５１３は空白にしている。これは検索者が部分一致検索を要求していることに相当する。勿論、名の入力欄５１３にもデータを入力しても良い。その場合には完全一致検索を要求していることになる。また、名の入力欄５１３だけにデータを設定した部分一致検索も可能である。

【００３４】検索者が検索キーの設定を終え、検索ボタン５１４によって検索を指示すると、検索装置３は図８に示す処理を開始する。

【００３５】先ず検索装置３の入出力部３１は、検索端末５の表示装置５１の検索画面５１１から検索キーなどの検索条件を入力する（Ｓ１１）。図７の検索画面５１

１による検索では、項目Ｃ２の検索キーとして指定された氏の入力欄５１２の「スズキ」と、名の入力欄５１３の値「空値」とを検索条件として入力する。次に、分解部３２は、入力された検索キーを単位文字に分解する（Ｓ１２）。ここでも、登録装置１の分解部１２と同様に、検索画面４１１に表示されている１文字を単位に分解する。従って、「スズキ」は「ス」、「ズ」、「キ」に分解される。

【００３６】次に暗号化部３３は、分解部３２で分解された個々の単位文字毎に独立に暗号化を行い、暗号化されたデータを元の単位文字の並びと同じ順に結合することで、暗号化検索キーを生成する。図９に単位文字に分解された「スズキ」を例に暗号化検索キーの生成の様子を示す。先ず、同図（ａ）に示すように、各単位文字毎に独立に暗号化し、各単位文字毎の暗号化データＢ、ｒ、ｇを生成する。次に、同図（ｂ）に示すように、暗号化データを結合し、「スズキ」に対応する暗号化検索キー「Ｂｒｇ」を生成する（Ｓ１３）。

【００３７】次に検索部３４は、暗号化部３３で生成された暗号化検索キーを受け取り、検索キーが「Ｂｒｇ」であり、検索対象項目がＣ２であり、部分一致検索であるといった検索条件を解析する（Ｓ１４）。そして、暗号化ファイル２に対して必要な検索を実行する（Ｓ１５）。つまり、前述した例では、暗号化ファイル２の各レコードの中から、項目Ｃ２中に暗号化検索キー「Ｂｒｇ」を含むレコードを検索する。検索部３４は、暗号化ファイル２から少なくとも１つのレコードの検索に成功した場合は（Ｓ１６でＹＥＳ）、取得したレコードを復号化部３５に渡す。

【００３８】復号化部３５は、渡されたレコード中の暗号化された項目Ｃ１、Ｃ２、Ｃｍを復号化する（Ｓ１７）。このとき、キー項目Ｃ１、Ｃ２については、単位文字毎に暗号化されたデータ毎に復号化を行い、復号化したデータを結合して、キー項目全体の復号化データを生成する。また、キー項目Ｃ１、Ｃ２以外の暗号化されている項目Ｃｍは項目全体を一括して復号化する。復号化部３５は、復号化したレコードを検索結果として、入出力部３１を通じて表示装置５１に出力する（Ｓ１８）。

【００３９】他方、検索部３４はレコードの検索に失敗した場合は（Ｓ１６でＮＯ）、該当レコード無しの検索結果を入出力部３１を通じて表示装置５１に出力する（Ｓ１８）。

【００４０】図１０は検索装置３で検索処理を行っている様子を模式的に示す。また、比較の為に、キー項目を暗号化せずに記録したファイルに対して検索する従来手法と、キー項目全体を一括に暗号化して記録した暗号化ファイルに対して検索キー全体を一括に暗号化した暗号化検索キーで検索する従来手法の模式図を図１１、図１２にそれぞれ示す。

【００４１】図１１では、「スズキ」を検索キーに、暗号化されていないファイルを検索しており、部分一致検索は可能であるが、ファイルが暗号化されていない為、セキュリティ性に問題がある。図１２では、「スズキ」全体を暗号化したデータ「３ｆ４」で暗号化ファイルを検索しているが、暗号化ファイルのキー項目は全体を一括して暗号化しているため、部分一致検索が行えない。

【００４２】これに対して本実施例では、図１０に示されるように、「スズキ」を「ス」、「ズ」、「キ」に分解して個別に暗号化し、それを結合した「Ｂｒｇ」で暗号化ファイルを検索しており、暗号化ファイルのキー項目も同様に、単位文字毎に暗号化したものを結合した暗号化データとなっているので、部分一致検索が可能となる。

【００４３】以上本発明の実施例について説明したが、本発明は以上の実施例にのみ限定されず、その他各種の付加変更が可能である。例えば、前記の実施例では、暗号化及び復号化に必要な鍵は暗号化ファイルシステム自体に予め設定されているものとしたが、暗号化ファイルシステムの外部で保持管理しておき、必要なときに暗号化ファイルシステムで利用する構成としたり、レコードの登録者やレコードの検索者がシステムに対して鍵を入力するよう構成しても良い。

【００４４】また、暗号化ファイル２に登録するレコードは、登録者の操作する登録端末４から逐次入力するものとしたが、登録対象となるレコードを磁気ディスク装置等の記憶装置に記憶しておき、その記憶されたレコードを登録装置１が読み込んで登録処理を行うようにしても良い。

【００４５】

【発明の効果】以上説明したように本発明によれば、ファイルにはキー項目のデータを単位文字毎に暗号化し結合して登録しておき、検索時には検索キーを単位文字毎に暗号化し結合した暗号化検索キーを用いてファイルを検索するので、暗号化された状態で部分一致検索が可能になる。これにより、部分一致検索をファイルのセキュリティ性を確保しながら実施することができる。

【図面の簡単な説明】

【図１】本発明の暗号化ファイルシステムの一例を示すブロック図である。

【図２】本発明の一実施例における暗号化ファイルの内容例を示す図である。

【図３】本発明の一実施例における登録装置の登録画面の一例を示す図である。

【図４】本発明の一実施例における登録装置の処理例を示すフローチャートである。

【図５】本発明の一実施例においてキー項目を単位文字に分解する方法の説明図である。

【図６】本発明の一実施例において単位文字毎に分解されたキー項目を暗号化する方法の説明図である。

11　　12

【図７】本発明の一実施例における検索装置の検索画面の一例を示す図である。
【図８】本発明の一実施例における検索装置の処理例を示すフローチャートである。
【図９】本発明の一実施例において検索キーを単位文字に分解して暗号化する方法の説明図である。
【図１０】本発明の一実施例における検索装置で検索処理を行っている様子を模式的に示す図である。
【図１１】キー項目を暗号化せずに記録したファイルに対して検索する従来技術の説明図である。
【図１２】キー項目全体を一括に暗号化して記録した暗号化ファイルに対して検索キー全体を一括に暗号化した暗号化検索キーで検索する従来技術の説明図である。
【符号の説明】
１…登録装置
＊２…暗号化ファイル
３…検索装置
４…登録端末
５…検索端末
６、７…記録媒体
１１…入力部
１２…分解部
１３…暗号化部
１４…登録部
３１…入出力部
３２…分解部
３３…暗号化部
３４…検索部
３５…復号化部

Fig 1　【図１】

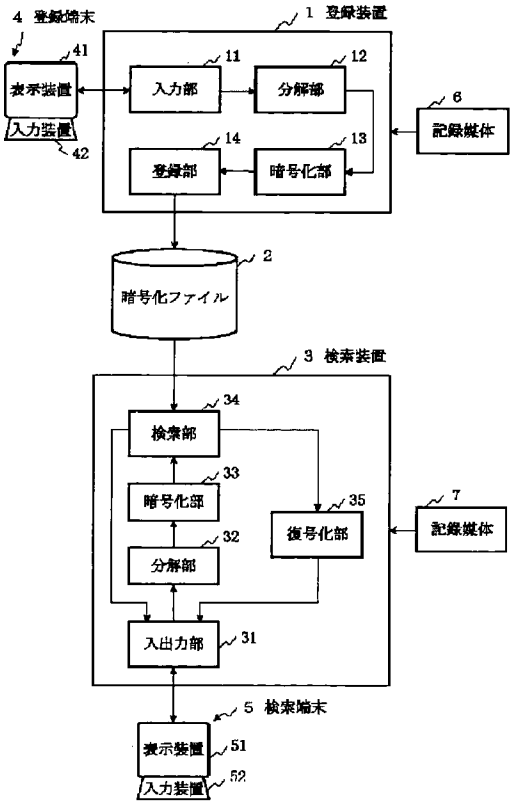


Fig 2　【図２】

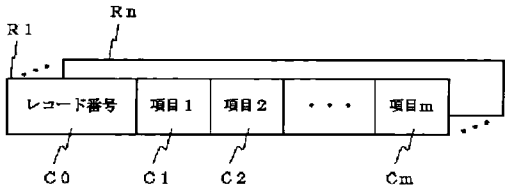


Fig 3　【図３】

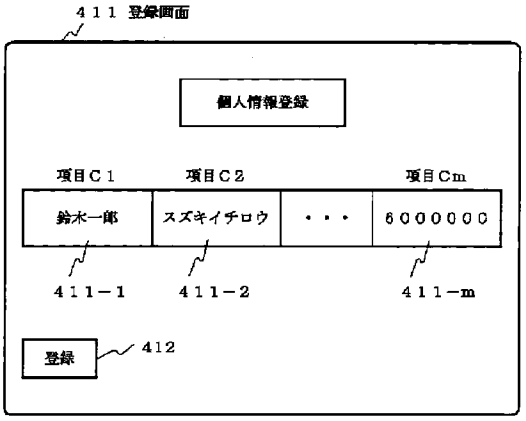


Fig 6　【図６】

(a)	「ス」	「ズ」	「キ」	「イ」	「チ」	「ロ」	「ウ」
	↓	↓	↓	↓	↓	↓	↓
	「B」	「r」	「g」	「e」	「a」	「¥」	「4」

(b)　Ｂｒｇｅａ¥４

Fig 9　【図９】

(a)	「ス」	「ズ」	「キ」
	↓	↓	↓
	「B」	「r」	「g」

(b)　Ｂｒｇ

Fig 4　【図４】

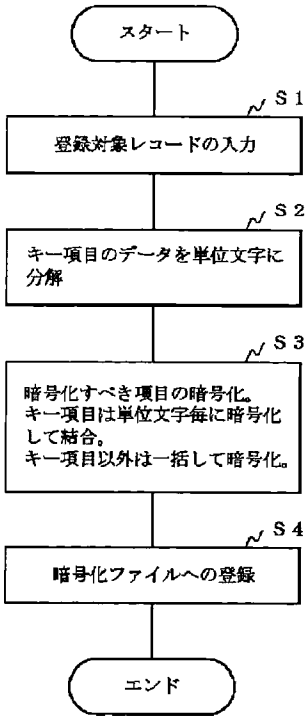


Fig 5　【図５】

(a)　鈴木一郎 →「鈴」、「木」、「一」、「郎」
　　スズキイチロウ →「ス」、「ズ」、「キ」、「イ」、「チ」、「ロ」、「ウ」

(b)　Ｈｅｎｒｙ →「H」、「e」、「n」、「r」、「y」

(c)　ä →「ä」

Fig 7　【図７】

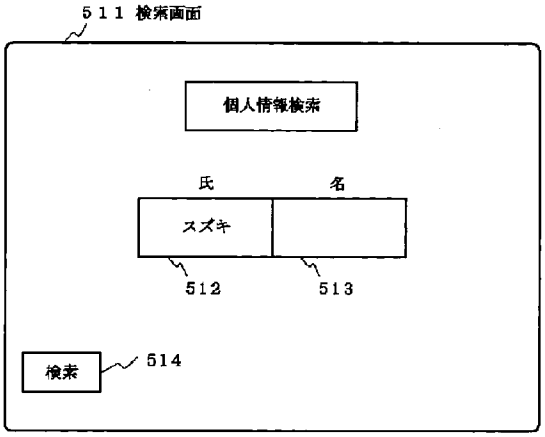


Fig 8　【図８】

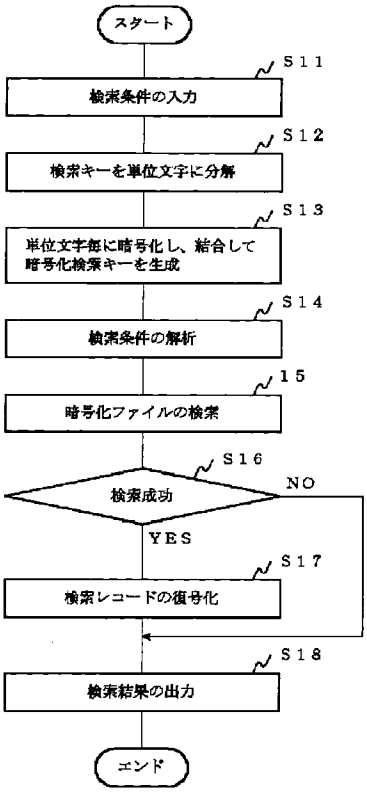


Fig 10

【図１０】

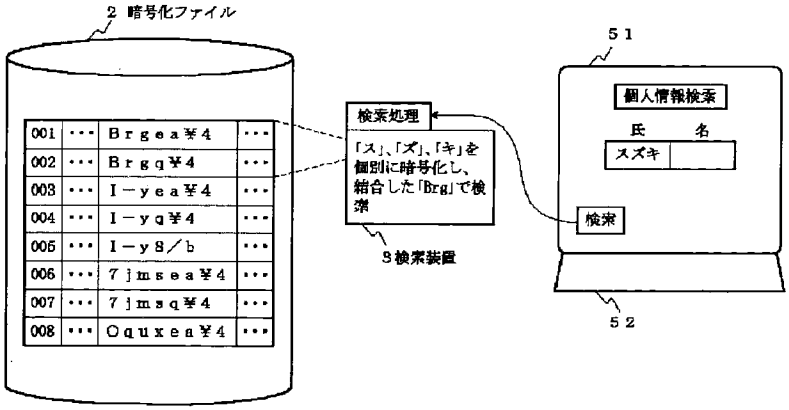


Fig 11

【図１１】

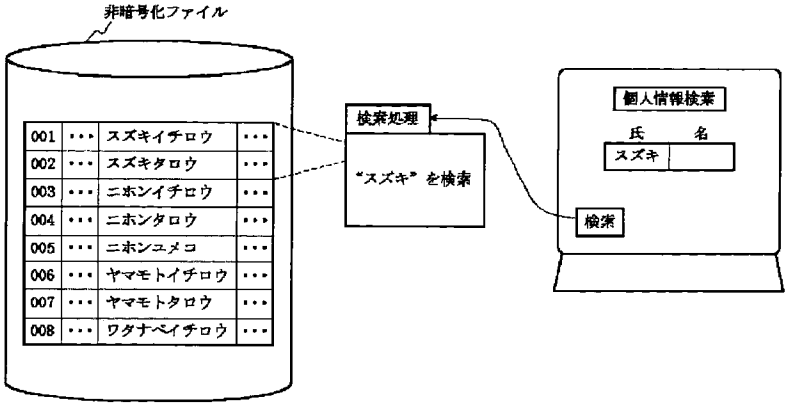


Fig 12

【図１２】